CLAIMS:

1. A key generation and distribution method for an authentication framework for an operator provider network and a service provider network comprising:

receiving a first request from a first requestor, the first request comprising an identity of the first requestor;

generating a new identity (ID) based on the identity of the first requestor;

generating a secret key based on an Identity Based Cryptography (IBC) key generation algorithm for the new ID and a pair of global keys comprising a Global Secret Key (GSK) and a Global Public Key (GPK);

transmitting the new ID, the secret key and the GPK to the first requestor;

receiving a request from a second requestor, the request comprising a plurality of identities;

generating a plurality of new IDs by generating an individual new ID for each of the plurality of identities;

generating a plurality secret keys based on the IBC key generation algorithm for each of the plurality of new IDs;

transmitting the plurality of new IDs, the plurality of secret keys corresponding to each of the plurality of IDs, and the GPK to the second requestor;

transmitting the plurality of new IDs and the plurality of secret keys to one or more other devices; and

performing mutual authentication between the one or more other devices and one of the first and second requestors.

2. The key generation and distribution method according to claim 1, wherein the step of generating the secret key based on the IBC key generation algorithm for the new ID and the pair of global keys comprises:

determining the pair of global keys from a plurality of pairs of global keys, and

generating the secret key for the new ID with the determined pair of global keys.

3. The key generation and distribution method according to claim 2, wherein the step of generating the secret key based on the IBC key generation algorithm for the new ID and the pair of global keys further comprises:

repeating the steps of determining the pair of global keys from the plurality of pairs of

global keys to determine a next pair of global keys from the plurality of pairs of global keys, and generating another secret key for the new ID to obtain a plurality of secret keys for the new ID.

4. The key generation and distribution method according to claim 3, wherein the step of transmitting the new ID, the secret key and the GPK to the first requestor further comprises:

transmitting a plurality of indexes associated with the pairs of global keys used for generating the secret keys.

5. The key generation and distribution method according to claim 1, wherein the step of generating the secret key based on the IBC key generation algorithm for each of the plurality of new IDs comprises:

determining the pair of global keys from a plurality of pairs of global keys, and

generating the secret key for the new ID with the determined pair of global keys.

6. The key generation and distribution method according to claim 5, wherein the step of generating the plurality of secret keys based on the IBC key generation algorithm for each of the plurality of new IDs further comprises:

repeating the steps of determining the pair of global keys from the plurality of pairs of global keys to determine a next pair of global keys from the plurality of pairs of global keys, and generating another secret key for each of the plurality of new IDs to obtain a plurality of secret keys for each of the plurality of new IDs.

7. The key generation and distribution method according to claim 3, wherein transmitting the plurality of new IDs, the secret keys corresponding to each of the plurality of IDs, and the GPK to the second requestor further comprises:

transmitting a plurality of indexes associated with the pairs of global keys used for generating the secret keys.

8. The key generation and distribution method according to claim 1, wherein the first requestor is a network authentication entity residing at the operator provider network and the second requestor is a Service Identity Management (IDM) entity residing at the service provider network.

9. The key generation and distribution method according to claim 1, wherein the new identity is generated by combining the identity of the first requestor and an index of the GPK.

10. The key generation and distribution method according to claim 1, wherein the secret key is generated by using the new identity and the pair of global keys together with the IBC key generation algorithm.

11. A key generation and distribution system for an authentication framework for an operating provider network comprising an authentication entity and a service provider network comprising an authentication server, the key generation and distribution system comprising:

a Network Identity Management (IDM), a User IDM and a Key Management Center (KMC) residing at the operating provider network; and

a Service IDM entity residing at the service provider network;

wherein the Network IDM comprises a processor, a memory, and instructions stored on the memory and executable by the processor to:

receive a request for credential from the authentication entity, the request comprising an identity of the authentication entity;

generate a new identity (ID) based on the identity of the authentication entity;

transmit the new ID to the KMC;

receive a secret key from the KMC; and

transmit the new ID and secret key to the authentication entity;

wherein the User IDM comprises a processor, a memory, and instructions stored on the memory and executable by the processor to:

receive a request for credentials from the Service IDM entity, the request comprising a plurality of identities;

generate a new identity (ID) for each of the plurality of identities;

transmit the new IDs to the KMC;

receive a plurality of secret keys from the KMC, each of the plurality of secret keys correspond to one of the plurality of identities; and

transmit the plurality of new IDs and plurality of secret keys to the Service IDM entity;

wherein the Service IDM entity comprises a processor, a memory, and instructions stored on the memory and executable by the processor to:

transmit a plurality of IDs to the User IDM;

receive the plurality of new IDs and the plurality of secret keys from the User IDM; and

distribute the plurality of new IDs and the plurality of secret keys to the authentication server and devices; and

wherein the KMC comprises a processor, a memory, and instructions stored on the memory and executable by the processor to:

receive the new ID from the Network IDM, generate the secret key, transmit the secret key to the Network IDM; and

receive the plurality of new IDs from the User IDM, generate the plurality of secret keys, transmit the plurality of secret keys to the Network IDM.

12. The key generation and distribution system according to claim 11, wherein the instructions of the KMC to receive the new ID from the Network IDM, generate the secret key, transmit the secret key to the Network IDM further comprises instructions executable by the processor to:

determine the pair of global keys from a plurality of pairs of global keys, and

generate the secret key for the new ID with the determined pair of global keys.

13. The key generation and distribution system according to claim 12, wherein the instructions of the KMC to receive the new ID from the Network IDM, generate the secret key, transmit the secret key to the Network IDM further comprises instructions executable by the processor to:

repeatedly determine the pair of global keys from the plurality of pairs of global keys to determine a next pair of global keys from the plurality of pairs of global keys, and generate another secret key for the new ID to obtain a plurality of secret keys for the new ID.

14. The key generation and distribution system according to claim 13, wherein the instructions of the KMC to receive the new ID from the Network IDM, generate the secret key, transmit the secret key to the Network IDM further comprises instructions executable by the processor to:

transmit a plurality of indexes associated with the pairs of global keys used for

generating the secret keys.

15. The key generation and distribution system according to claim 11, wherein the instructions of the KMC to receive the plurality of new IDs from the User IDM, generate the plurality of secret keys, transmit the plurality of secret keys to the Network IDM further comprises instructions executable by the processor to:

determine the pair of global keys from a plurality of pairs of global keys; and

generate the secret key for the new ID with the determined pair of global keys.

16. The key generation and distribution system according to claim 15, wherein the instructions of the KMC to receive the plurality of new IDs from the User IDM, generate the plurality of secret keys, transmit the plurality of secret keys to the Network IDM further comprises instructions executable by the processor to:

repeatedly determine the pair of global keys from the plurality of pairs of global keys to determine a next pair of global keys from the plurality of pairs of global keys, and generate another secret key for each of the plurality of new IDs to obtain a plurality of secret keys for each of the plurality of new IDs.

17. The key generation and distribution system according to claim 16, wherein the instructions of the KMC to receive the plurality of new IDs from the User IDM, generate the plurality of secret keys, transmit the plurality of secret keys to the Network IDM further comprises instructions executable by the processor to:

transmit a plurality of indexes associated with the pairs of global keys used for generating the secret keys.

18. The key generation and distribution system according to claim 11, wherein the new ID is generated by combining the identity received and an expiry date of the identity.

19. The key generation and distribution system according to claim 11, wherein the secret key is generated by the KMC by using the new identity and a predetermined pair of global keys comprising a Global Public Key (GPK) and a Global Secret Key (GSK) together with an Identity Based Cryptography (IBC) key generation algorithm.